We claim:

1. A system for providing improved audio compression, comprising:

a security core which provides security functions;

one or more components, comprising at least an audio recording component and one or more transformation components;

means for operating the security core;

means for securely operably connecting the components to the security core, such that the security core can vouch for authenticity of each securely operably connected component;

means for recording an audio stream by the securely operably connected audio recording component;

means for transforming the audio stream to a text stream by at least one of the securely operably connected transformation components; and

means for securely providing, for the text stream by the security core, an identification of the securely operably connected audio recording component and each of the at least one securely operably connected transformation components.

2. The system according to Claim 1, wherein selected ones of the operable connections are made using one or more buses of the security core.

3. The system according to Claim 1, wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security core.

4. The system according to Claim 3, wherein the wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key.

5. The system according to Claim 1, wherein selected ones of the secure operable connections are provided when the security core is manufactured.

6. The system according to Claim 1, wherein the means for securely operably connecting further comprises means for authenticating the operably connected component to the security core.

7. The system according to Claim 6, wherein the means for authenticating further comprises:

means for providing a unique identifier of the operably connected component to the security core, along with a digital signature of the unique identifier that is created using a private key of the operably connected component; and

means for using, by the security core, a public key that is cryptographically associated with the private key to determine authenticity of the operably connected component.

8. The system according to Claim 1, wherein the means for securely operably connecting is activated by a hardware reset of the component, and wherein the hardware reset is activated by operably connecting of the component.

9. The system according to Claim 6, wherein the means for authenticating are securely stored on the operably connected component.

10. The system according to Claim 6, further comprising means for authenticating the security core to the operably connected component.

11. The system according to Claim 1, further comprising:

means for detecting whether the audio recording component and the at least one transformation component remain operably connected to the security core during operation of the means for recording and the means for transforming; and

means for aborting the recording or the transforming if one or more of the audio recording component and the at least one transformation component fails to remain operably connected to the security core during operation of the means for recording and the means for transforming.

12. The system according to Claim 1, further comprising:

means for detecting whether the audio recording component and the at least one transformation component remain operably connected to the security core during operation of the means for recording and the means for transforming; and means for marking the text stream as not authenticated if one or more of the audio recording component and the at least one transformation component fails to remain operably connected to the security core during operation of the means for recording and the means for transforming.

13. The system according to Claim 7, further comprising:

means for determining whether the audio recording component and the at least one transformation component have been authenticated to the security core; and

means for aborting the recording or the transforming if one or more of the audio recording component and the at least one transformation component has not been authenticated to the security core.

14. The system according to Claim 7, further comprising:

means for determining whether the audio recording component and the at least one transformation component have been authenticated to the security core; and

means for marking the text stream as not authenticated if one or more of the audio recording component and the at least one transformation component has not been authenticated to the security core.

15. The system according to Claim 1, wherein the means for securely providing further comprises means for digitally notarizing, by the security core, the text stream.

16. The system according to Claim 1, wherein the means for securely providing further comprises means for providing an additional data stream that is associated with the text stream, wherein the additional data stream comprises a digital notarization, created by the security core, of the text stream.

17. The system according to Claim 15, wherein the means for digitally notarizing further comprises:

means for computing, by the security core, a hash value over the text stream;

means for combining the hash value with a unique identifier of the audio recording component and of each of the at least one transformation components, thereby creating a combination data block;

means for hashing the combination data block;

means for digitally signing the hashed combination data block with a private cryptographic key of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith; and

means for providing the digitally signed hashed combination data block, along with the combination data block, as the digital notarization for the text stream, wherein the digital notarization cryptographically seals contents of the text stream and identifies the audio recording component and each of the at least one transformation components.

18. The system according to Claim 17, further comprising means for verifying authenticity of the text stream by a receiver of the text stream and the digital notarization, using the public

cryptographic key of the security core, and for concluding that the text stream is authentic if the verification succeeds.

19. The system according to Claim 18, wherein the means for verifying authenticity further comprises concluding that the text stream has not been tampered with if the verification succeeds.

20. The system according to Claim 18, wherein the means for verifying authenticity further comprises means for determining the audio recording component and the at least one transformation component involved in creating the text stream by decoding the digitally signed hashed combination data block to reveal the unique identifiers thereof.

21. The system according to Claim 15, wherein:

the means for transforming the audio stream to a text stream further comprises:

means for transforming the audio stream to a digital stream by a first of the at least one transformation components which is an analog-to-digital transformation component; and

means for converting the digital stream to the text stream by a second of the at least one transformation components which is a voice recognition transformation component; and

the means for digitally notarizing the text stream further comprises:

means for computing a hash over the text stream;

means for combining the hash with unique identifiers of the audio recording component, the analog-to-digital transformation component, and the voice recognition transformation component; and means for digitally signing the combination using a private cryptographic key of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith.

22. The system according to Claim 15, wherein:

the means for transforming the audio stream to a text stream further comprises:

means for transforming the audio stream to a first digital stream by a first of the at least one transformation components which is an analog-to-digital transformation component;

means for converting the first digital stream to a first encoded text stream by a second of the at least one transformation components which is a voice recognition transformation component, wherein the voice recognition transformation component may be augmented by zero or more others of the at least one transformation components which are an authenticated speaker-specific voice recognition database and/or a lexical transformation component; and

means for compressing the first encoded text stream into the text stream using a third of the at least one transformation components which is a text compression transformation component; and

the means for digitally notarizing the text stream further comprises:

means for computing a hash over the text stream;

means for combining the hash with unique identifiers of: (1) the audio recording component; (2) the analog-to-digital transformation component; (3) the voice recognition transformation component; (4) the authenticated speaker-specific voice recognition database and/or the lexical transformation component, if they augmented the voice recognition transformation component; (5) the text compression transformation component; and

means for signing the combination using a private cryptographic key of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith.

23. The system according to Claim 1, wherein the text stream is an ASCII text stream.

24. The system according to Claim 1, wherein the text stream is an EBCDIC text stream.

25. A method of providing improved audio compression, comprising steps of:

operating a security core which provides security functions;

providing one or more components, comprising at least an audio recording component and one or more transformation components;

securely operably connecting the components to the security core, such that the security core can vouch for authenticity of each securely operably connected component;

recording an audio stream by the securely operably connected audio recording component;

transforming the audio stream to a text stream by at least one of the securely operably connected transformation components; and

securely providing, for the text stream by the security core, an identification of the securely operably connected audio recording component and each of the at least one securely operably connected transformation components.

26. The method according to Claim 25, wherein selected ones of the operable connections are made using one or more buses of the security core.

27. The method according to Claim 25, wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security core.

28. The method according to Claim 27, wherein the wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key.

29. The method according to Claim 25, wherein selected ones of the secure operable connections are provided when the security core is manufactured.

30. The method according to Claim 25, wherein the step of securely operably connecting further comprises the step of authenticating the operably connected component to the security core.

31. The method according to Claim 30, wherein the authenticating step further comprises steps of:

providing a unique identifier of the operably connected component to the security core, along with a digital signature of the unique identifier that is created using a private key of the operably connected component; and

using, by the security core, a public key that is cryptographically associated with the private key to determine authenticity of the operably connected component.

32. The method according to Claim 25, wherein the step of securely operably connecting is activated by a hardware reset of the component, and wherein the hardware reset is activated by operably connecting of the component.

33. The method according to Claim 30, wherein instructions for performing the authenticating step are securely stored on the operably connected component.

34. The method according to Claim 30, further comprising the step of authenticating the security core to the operably connected component.

35. The method according to Claim 25, further comprising steps of:

detecting whether the audio recording component and the at least one transformation component remain operably connected to the security core during operation of the recording step and the transforming step; and aborting the recording or the transforming if one or more of the audio recording component and the at least one transformation component fails to remain operably connected to the security core during operation of the recording step and the transforming step.

36. The method according to Claim 25, further comprising steps of:

detecting whether the audio recording component and the at least one transformation component remain operably connected to the security core during operation of the recording step and the transforming step; and

marking the text stream as not authenticated if one or more of the audio recording component and the at least one transformation component fails to remain operably connected to the security core during operation of the recording step and the transforming step.

37. The method according to Claim 31, further comprising steps of:

determining whether the audio recording component and the at least one transformation component have been authenticated to the security core; and

aborting the recording or the transforming if one or more of the audio recording component and the at least one transformation component has not been authenticated to the security core.

38. The method according to Claim 31, further comprising steps of:

determining whether the audio recording component and the at least one transformation component have been authenticated to the security core; and marking the text stream as not authenticated if one or more of the audio recording component and the at least one transformation component has not been authenticated to the security core.

39. The method according to Claim 25, wherein the step of securely providing further comprises the step of digitally notarizing, by the security core, the text stream.

40. The method according to Claim 25, wherein the step of securely providing further comprises the step of providing an additional data stream that is associated with the text stream, wherein the additional data stream comprises a digital notarization, created by the security core, of the text stream.

41. The method according to Claim 39, wherein the digitally notarizing step further comprises steps of:

computing, by the security core, a hash value over the text stream;

combining the hash value with a unique identifier of the audio recording component and of each of the at least one transformation components, thereby creating a combination data block;

hashing the combination data block;

digitally signing the hashed combination data block with a private cryptographic key of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith; and providing the digitally signed hashed combination data block, along with the combination data block, as the digital notarization for the text stream, wherein the digital notarization cryptographically seals contents of the text stream and identifies the audio recording component and each of the at least one transformation components.

42. The method according to Claim 41, further comprising the step of verifying authenticity of the text stream by a receiver of the text stream and the digital notarization, using the public cryptographic key of the security core, and concluding that the text stream is authentic if the verification succeeds.

43. The method according to Claim 42, wherein the step of verifying authenticity further comprises concluding that the text stream has not been tampered with if the verification succeeds.

44. The method according to Claim 42, wherein the step of verifying authenticity further comprises the step of determining the audio recording component and the at least one transformation component involved in creating the text stream by decoding the digitally signed hashed combination data block to reveal the unique identifiers thereof.

45. The method according to Claim 39, wherein:

the step of transforming the audio stream to a text stream further comprises steps of:

transforming the audio stream to a digital stream by a first of the at least one transformation components which is an analog-to-digital transformation component; and converting the digital stream to the text stream by a second of the at least one transformation components which is a voice recognition transformation component; and

the step of digitally notarizing the text stream further comprises steps of:

computing a hash over the text stream;

combining the hash with unique identifiers of the audio recording component, the analog-to-digital transformation component, and the voice recognition transformation component; and

digitally signing the combination using a private cryptographic key of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith.

46. The method according to Claim 39, wherein:

the step of transforming the audio stream to a text stream further comprises steps of:

transforming the audio stream to a first digital stream by a first of the at least one transformation components which is an analog-to-digital transformation component;

converting the first digital stream to a first encoded text stream by a second of the at least one transformation components which is a voice recognition transformation component, wherein the voice recognition transformation component may be augmented by zero or more others of the at least one transformation components which are an authenticated speaker-specific voice recognition database and/or a lexical transformation component; and compressing the first encoded text stream into the text stream using a third of the at least one transformation components which is a text compression transformation component; and

the step of digitally notarizing the text stream further comprises steps of:

computing a hash over the text stream;

combining the hash with unique identifiers of: (1) the audio recording component; (2) the analog-to-digital transformation component; (3) the voice recognition transformation component; (4) the authenticated speaker-specific voice recognition database and/or the lexical transformation component, if they augmented the voice recognition transformation component; (5) the text compression transformation component; and

signing the combination using a private cryptographic key of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith.

47. The method according to Claim 25, wherein the text stream is an ASCII text stream.

48. The method according to Claim 25, wherein the text stream is a Unicode text stream.

49. A computer program product for providing improved audio compression, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for operating a security core which provides security functions;

computer-readable program code means for securely operably connecting one or more components, comprising at least an audio recording component and one or more transformation components, to the security core, such that the security core can vouch for authenticity of each securely operably connected component;

computer-readable program code means for transforming an audio stream that is recorded by the securely operably connected audio recording component to a text stream, the transforming being performed by at least one of the securely operably connected transformation components; and

computer-readable program code means for securely providing, for the text stream by the security core, an identification of the securely operably connected audio recording component and each of the at least one securely operably connected transformation components.

50. The computer program product according to Claim 49, wherein selected ones of the operable connections are made using one or more buses of the security core.

51. The computer program product according to Claim 49, wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security core.

52. The computer program product according to Claim 51, wherein the wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage

of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key.

53. The computer program product according to Claim 49, wherein selected ones of the secure operable connections are provided when the security core is manufactured.

54. The computer program product according to Claim 49, wherein the computer-readable program code means for securely operably connecting further comprises computer-readable program code means for authenticating the operably connected component to the security core.

55. The computer program product according to Claim 54, wherein the computer-readable program code means for authenticating further comprises:

computer-readable program code means for providing a unique identifier of the operably connected component to the security core, along with a digital signature of the unique identifier that is created using a private key of the operably connected component; and

computer-readable program code means for using, by the security core, a public key that is cryptographically associated with the private key to determine authenticity of the operably connected component.

56. The computer program product according to Claim 49, wherein the computer-readable program code means for securely operably connecting is activated by a hardware reset of the

component, and wherein the hardware reset is activated by operably connecting of the component.

57. The computer program product according to Claim 54, wherein the computer-readable program code means for authenticating are securely stored on the operably connected component.

58. The computer program product according to Claim 54, further comprising computer-readable program code means for authenticating the security core to the operably connected component.

59. The computer program product according to Claim 49, further comprising:

computer-readable program code means for detecting whether the audio recording component and the at least one transformation component remain operably connected to the security core during operation of the recording and the computer-readable program code means for transforming; and

computer-readable program code means for aborting the recording or the transforming if one or more of the audio recording component and the at least one transformation component fails to remain operably connected to the security core during operation of the recording and the computer-readable program code means for transforming.

60. The computer program product according to Claim 49, further comprising:

computer-readable program code means for detecting whether the audio recording component and the at least one transformation component remain operably connected to the security core during operation of the recording and the computer-readable program code means for transforming; and

computer-readable program code means for marking the text stream as not authenticated if one or more of the audio recording component and the at least one transformation component fails to remain operably connected to the security core during operation of the recording and the computer-readable program code means for transforming.

61. The computer program product according to Claim 55, further comprising:

computer-readable program code means for determining whether the audio recording component and the at least one transformation component have been authenticated to the security core; and

computer-readable program code means for aborting the recording or the transforming if one or more of the audio recording component and the at least one transformation component has not been authenticated to the security core.

62. The computer program product according to Claim 55, further comprising:

computer-readable program code means for determining whether the audio recording component and the at least one transformation component have been authenticated to the security core; and computer-readable program code means for marking the text stream as not authenticated if one or more of the audio recording component and the at least one transformation component has not been authenticated to the security core.

63. The computer program product according to Claim 49, wherein the computer-readable program code means for securely providing further comprises computer-readable program code means for digitally notarizing, by the security core, the text stream.

64. The computer program product according to Claim 49, wherein the computer-readable program code means for securely providing further comprises computer-readable program code means for providing an additional data stream that is associated with the text stream, wherein the additional data stream comprises a digital notarization, created by the security core, of the text stream.

65. The computer program product according to Claim 63, wherein the computer-readable program code means for digitally notarizing further comprises:

computer-readable program code means for computing, by the security core, a hash value over the text stream;

computer-readable program code means for combining the hash value with a unique identifier of the audio recording component and of each of the at least one transformation components, thereby creating a combination data block;

computer-readable program code means for hashing the combination data block;

computer-readable program code means for digitally signing the hashed combination data block with a private cryptographic key of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith; and

computer-readable program code means for providing the digitally signed hashed combination data block, along with the combination data block, as the digital notarization for the text stream, wherein the digital notarization cryptographically seals contents of the text stream and identifies the audio recording component and each of the at least one transformation components.

66. The computer program product according to Claim 65, further comprising computer-readable program code means for verifying authenticity of the text stream by a receiver of the text stream and the digital notarization, using the public cryptographic key of the security core, and for concluding that the text stream is authentic if the verification succeeds.

67. The computer program product according to Claim 66, wherein the computer-readable program code means for verifying authenticity further comprises concluding that the text stream has not been tampered with if the verification succeeds.

68. The computer program product according to Claim 66, wherein the computer-readable program code means for verifying authenticity further comprises computer-readable program code means for determining the audio recording component and the at least one transformation

component involved in creating the text stream by decoding the digitally signed hashed combination data block to reveal the unique identifiers thereof.

69. The computer program product according to Claim 63, wherein:

the computer-readable program code means for transforming the audio stream to a text stream further comprises:

computer-readable program code means for transforming the audio stream to a digital stream by a first of the at least one transformation components which is an analog-to-digital transformation component; and

computer-readable program code means for converting the digital stream to the text stream by a second of the at least one transformation components which is a voice recognition transformation component; and

the computer-readable program code means for digitally notarizing the text stream further comprises:

computer-readable program code means for computing a hash over the text stream;

computer-readable program code means for combining the hash with unique identifiers of the audio recording component, the analog-to-digital transformation component, and the voice recognition transformation component; and

computer-readable program code means for digitally signing the combination using a private cryptographic key of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith.

70. The computer program product according to Claim 63, wherein:

the computer-readable program code means for transforming the audio stream to a text stream further comprises:

computer-readable program code means for transforming the audio stream to a first digital stream by a first of the at least one transformation components which is an analog-to-digital transformation component;

computer-readable program code means for converting the first digital stream to a first encoded text stream by a second of the at least one transformation components which is a voice recognition transformation component, wherein the voice recognition transformation component may be augmented by zero or more others of the at least one transformation components which are an authenticated speaker-specific voice recognition database and/or a lexical transformation component; and

computer-readable program code means for compressing the first encoded text stream into the text stream using a third of the at least one transformation components which is a text compression transformation component; and

the computer-readable program code means for digitally notarizing the text stream further comprises:

computer-readable program code means for computing a hash over the text stream;

computer-readable program code means for combining the hash with unique identifiers of: (1) the audio recording component; (2) the analog-to-digital transformation component; (3) the voice recognition transformation component; (4) the authenticated speaker-specific voice recognition database and/or the lexical transformation component, if they augmented the voice recognition transformation component; (5) the text compression transformation component; and

computer-readable program code means for signing the combination using a private cryptographic key of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith.

71. The computer program product according to Claim 49, wherein the text stream is an ASCII text stream.

72. The computer program product according to Claim 49, wherein the text stream is a Unicode text stream.